ABSTRACT:

A transmitter 100 provides receivers 120 conditional access to data transmitted via a network. A content encryptor 210 is used to encrypt the data under control of a same authorization key before it is transmitted to all receivers. The transmitter has a storage 100 with a plurality of device keys. A further encryptor 270 is used for producing a key block with a plurality of entries, where each entry is associated with a respective one of the device keys. At least some of the entries contain a representation of the authorization key encrypted with the associated device key. The transmitter transmits the same key block to all receivers.

The receiver 120 has a subset of the device keys. A first decryptor 272 is used to retrieve the authorization key by decrypting at least one entry of the key block that is associated with one of the device keys of the receiver. A second decryptor 240 is used for decrypting the data under control of the authorization key.

Fig. 3